IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JENNIFER MILLER, SCOTT POOLE, and KEVIN ENGLUND	)	
Plaintiffs,	)	No. 1:18-CV-00086
v.	)	Hon. Marvin E. Aspen
SOUTHWEST AIRLINES CO., a Texas corporation,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Jennifer Miller, Scott Poole, and Kevin Englund ("Plaintiffs"), individually and on behalf of other similarly situated individuals, bring this Amended Class Action Complaint against Defendant Southwest Airlines Co. ("Southwest" or "Defendant"), to stop Defendant's capture, collection, use, and storage of individuals' biometric identifiers and/or biometric information in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. ("BIPA") and the common law, and to obtain redress for all persons injured by Defendant's conduct. Plaintiffs allege as follows based on personal knowledge as to their own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by their attorneys.

INTRODUCTION

1. This case concerns an international commercial airline capturing, collecting, storing, and using Plaintiffs' and other workers' biometric identifiers

and/or biometric information without regard to BIPA, the common law, and the concrete privacy rights and pecuniary interests those laws protect here.

2. Specifically, Defendant implemented, without consent, an invasive timekeeping program of capturing, collecting, storing, and using Plaintiffs' and other Southwest employees' fingerprints. Defendant uses employees' fingerprint scans to identify such employees for timekeeping and payroll purposes.

3. The nature of the substantive privacy interests at issue here has been recognized by the Illinois legislature pursuant to BIPA. In addition, the Federal Trade Commission and numerous privacy experts have also recognized the substantive privacy interests at issue as well as the resultant injury when those interests are violated. Moreover, expert studies show that such injuries can be quantified in dollars and cents.

4. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in capturing, collecting, storing, and using Plaintiffs' and other similarly situated individuals' biometric identifiers and biometric information without notice or informed written consent, in direct violation of the Illinois' BIPA and the common law.

PARTIES

5. Defendant Southwest Airlines Co. is a foreign corporation incorporated under the laws of the State of Texas, and having its principal place of business in Dallas, Texas. At all times relevant to this Complaint, Southwest Airlines Co. was

registered with and authorized by the Illinois Secretary of State to transact business in Illinois, and transacting business in Cook County, Illinois.

6. At all relevant times, Plaintiff Jennifer Miller has been a resident of Romeoville, Illinois and citizen of the State of Illinois. She has worked as a ramp agent and operations agent for Southwest at Chicago Midway International Airport since 2005.

7. At all relevant times, Plaintiff Scott Poole has been a resident of Crestwood, Illinois and citizen of the State of Illinois. He has worked as a ramp agent for Southwest at Chicago Midway International Airport since 2009.

8. At all relevant times, Plaintiff Kevin Englund has been a resident of Alsip, Illinois and citizen of the State of Illinois. He has worked as a ramp agent for Southwest at Chicago Midway International Airport since 2007.

JURISDICTION AND VENUE

9. This Court has diversity jurisdiction under 28 U.S.C. § 1332(d) because: (i) at least one member of the putative class is a citizen of a state different from any Defendant; (ii) the amount in controversy exceeds $5,000,000 exclusive of interest and costs; and (iii) none of the exceptions under that subsection apply to this action.

10. This Court has personal jurisdiction over Defendant because Defendant transacts business in Illinois and a substantial part of the events giving rise to Plaintiffs' claims arise out of Defendant's unlawful in-state actions, as Defendant captured Plaintiffs' biometrics in this State.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District, as Defendant captured Plaintiffs' biometrics at one of the facilities located in this District.

BACKGROUND

I. BIPA Was Enacted To Protect Persons' Most Sensitive, Immutable Personal Information

12. Following the 2007 bankruptcy of a company specializing in the collection and use of biometric information, which risked the sale or transfer of millions of fingerprint records to the highest bidder, the Illinois legislature enacted BIPA to regulate the collection, use, and retention of biometric information by private entities.

13. The Illinois Legislature recognized that the sensitivity of biometric information was in a class of its own: "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. [E]ven sensitive information like Social Security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to each individual and cannot be changed, and therefore, once compromised, such individual has no recourse, is at a heightened risk for identity theft, and is likely to withdraw from biometric facilitated transactions." 740 ILCS 14/5.

14. To effectuate persons' substantive privacy interest in their unique, immutable biometric information, BIPA provides that private entities may not obtain and/or possess an individual's biometrics unless they first:

(1) inform that person in writing that biometric identifiers or information will be collected or stored;

(2) inform that person in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being collected, stored and used;

(3) receive a written release from the person for the collection of their biometric identifiers or biometric information; and

(4) publish a publicly available retention schedule and guidelines for permanently destroying biometric identifiers and biometric information.

740 ILCS 14/5.

15. BIPA recognizes that without notice and consent, persons are unaware of the nature and extent of the sensitive personal information companies collect from them and use to the companies' benefit. BIPA acknowledges persons' substantive privacy right in biometric information and protects such right from encroachment by private companies.

16. BIPA broadly defines the biometrics to which it applies. Under the Act, a "biometric identifier" is any personal feature that is unique to an individual and includes fingerprints, facial scans, iris scans, palm scans, and DNA, among others. "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier which is used to identify an individual. 740 ILCS 14/10.

17. The enactment of BIPA was prescient. Today, many businesses and financial institutions have incorporated biometric applications into their consumer products, including such ubiquitous consumer products as checking accounts and cell

phones. Moreover, the usage of biometrics has been incorporated into the labor and employment side of commerce for timekeeping purposes, as is the case here.

18. As the recent Equifax Data Breach and others have made clear, electronically stored information ("ESI") is notoriously difficult to protect and its dissemination can have disastrous consequences. The inherent difficulty in protecting ESI, combined with the uniquely irreplaceable nature of biometric information, means that the privacy risks associated with a person's biometrics are unparalleled. Such information is far more sensitive than a Social Security number, passport, birth certificate, or similar sensitive personal information.

II. BIPA Creates a Private Right of Action Against Any Entity That Collects Biometric Information Without Providing Notice and Obtaining Written Consent

19. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, and use biometrics and creates a private right of action for lack of statutory compliance.

20. Indeed, at the time BIPA was passed in 2008, another data privacy statute, the Personal Information Protection Act, 815 ILCS 530 *et seq*. ("PIPA"), had already been enacted in Illinois since 2006. PIPA provides a private right of action if a company possessing an individual's unique biometric data (the same data regulated by BIPA) suffers a data security breach and fails to give affected consumers proper notice of such a breach.

21. Because it believed PIPA provided insufficient protection to individuals regarding their highly sensitive biometrics, the Illinois legislature passed BIPA to expand the law to cover not only data breach cases, but also to regulate the initial collection, use, storage, and dissemination of such biometrics and the publication of information relating to same.

22. BIPA is narrowly tailored with provisions that do not place an absolute bar on the collection, capture, or dissemination of biometrics. For companies wishing to comply with BIPA, such compliance is straightforward. The necessary disclosures and a written release can be easily achieved through a single, signed sheet of paper. BIPA's requirements simply bestow on consumers a right to privacy in their biometrics and a right to make an informed decision when electing to provide or withhold their most sensitive information and on what terms.

III. Southwest Has for Years Subjected Employees to a Biometric Timekeeping System Without Providing Notice or Obtaining Consent

23. Most businesses track workers' time using traditional methods that do not collect or capture workers' biometric information.

24. Such methods can be less profitable as they cannot guarantee that mistakes are not made with respect to recording employee time or that time records are not falsified.

25. Biometric timekeeping mechanisms, on the other hand, better ensure the accuracy of employee time records because they require a person's unique,

immutable biometric characteristics. As such, biometric timekeeping mechanisms save companies significant amounts of money.

26. Because of the cost-savings, Defendant elected to implement a biometric time-tracking program in lieu of less invasive—but also less profitable—timekeeping mechanisms.

27. Under Defendant's timekeeping method, Defendant's employees are required to provide their biometric information—namely, their fingerprints—to Defendant as a condition of their employment. Defendant's employees must then scan their fingers to "clock-in" and "clock-out" of work every day. Accordingly, as a part of Defendant's timekeeping system, Defendant captures, collects, stores, and uses its workers' fingerprints to identify them in the future for timekeeping and payroll purposes.

28. A worker's fingerprint scan is a distinctive identifier and constitutes a biometric identifier and biometric information under BIPA.

29. Despite Defendant's capture, collection, storage, and use of its employees' fingerprints through this system, Defendant did not provide, and has never provided, the requisite notice regarding its biometric timekeeping program. Moreover, Defendant did not obtain, and has never obtained, informed written consent from its employees who are required to use the biometric timekeeping system. Defendant has also never published data retention and deletion policies for its employees.

30. Defendant still retains its employees' biometric information. Such retention is an unlawful and continuing infringement of employees' right to privacy in their biometric identifiers and biometric information.

31. Defendant's conduct is particularly unsettling considering the economic benefit and fraud-prevention it obtains from its biometric timekeeping system, while wholly avoiding any costs associated with implementing such systems in compliance with the law. This cognizable benefit is not only to the detriment of its workers, but also to its law-abiding competitors who comply with BIPA.

32. Furthermore, Defendant's unlawful actions expose workers to serious and irreversible privacy risks—risks that BIPA was designed to avoid—including the ever-present risk of a data breach of Defendant's systems exposing its employees' biometrics to hackers and other wrongdoers worldwide.

33. The risk to workers as a result of Defendant's actions is compounded when, as here, workers' biometric information is associated with his/her Social Security number and potentially other relevant financial information. The gravity of the unresolvable problems created in the event of a biometric data breach is so severe that the unlawful collection and/or dissemination of such information constitutes actual harm.

34. As the Illinois legislature acknowledged in enacting BIPA, persons like Plaintiffs should not have to wait until their immutable personal characteristics are stolen by criminals to have a right to pursue a claim to protect their privacy interests.

IV. Defendant's BIPA Violations Have Caused Quantifiable Injury

35. The Federal Trade Commission ("FTC") and numerous privacy experts have recognized the concrete injury caused by privacy violations BIPA was designed to prevent.

36. In particular, the FTC recently hosted a workshop to discuss privacy harms characterized as "informational injury."[1] Persons suffer informational injury when personal information about them is illegally obtained or misused, as is the case when a company violates BIPA.

37. The FTC held the workshop because of the growing use of consumer personal information by private companies. The FTC believes that such companies' behavior requires that the FTC recognize and quantify the injury that results from the unlawful acquisition or use of personal data, particularly injury beyond the obvious financial ones (such as credit card theft) that privacy intrusions can cause. Indeed, acting FTC Chairman, Maureen Olhausen, emphasized in her opening remarks that "we need to examine more thoroughly the range of injuries that can occur from privacy and data security events[,]" including "unwarranted health and safety risk and intrusion into seclusion."[2]

38. Leading privacy experts similarly recognize injury different from direct financial injury that privacy violations can cause.

---

[1] FTC Informational Injury Workshop (Dec. 12, 2017), *available at* https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop (last visited Apr. 2, 2018).
[2] *Id.* (Opening Remarks), *available at* https://www.ftc.gov/news-events/audio-video/video/informational-injury-opening-remarks (last visited Apr. 2, 2018).

39. For example, Michelle De Mooy, Director of the Data & Privacy Project at the Center for Democracy and Technology, opined during the FTC's workshop that injury occurs when a pharmacy tracks customer purchasing behavior without notice or consent because, in the privacy context, "expectations [and consent] matter. So when you walk into a pharmacy [or any kind of store] . . . most of us . . . don't have the expectation that our phones will be pinged repeatedly by a tracking system. Also, the idea of whether or not [the customer] was asked for consent [is important]."[3]

40. Similarly, economic and privacy professionals Sarah Butler and Garrett Glasgow, Ph.D. have explained that "[i]n the privacy setting, an individual's 'existence value' comes from the knowledge that their personal data is secure and untouched by unauthorized third parties, and damages arise when an individual discovers this is no longer true, even if there is no direct financial harm from the data sharing or data breach."[4]

41. Injury resulting from the unwanted collection, storage, and/or use of personal information can be quantified in dollars and cents. Butler and Glasgow have demonstrated as much through the use of "a discrete choice experiment—a specialized type of survey which asks consumers to evaluate products that are 'bundles' of attributes [including attributes related to the product provider's collection and use of personal information] and make decisions about the most preferred

[3] *Id.* (Panel 4 – Measuring Injury), *available at* https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-4-measuring-injury (last visited Apr. 2, 2018).
[4] Sarah Butler & Garret Glasgow, Ph.D., "Damages Based On The Intrinsic Value Of Privacy?" Law360 (July 8, 2015), *available at* http://www.nera.com/content/dam/nera/publications/2015/Damages%20Based%20On%20The%20Intrinsic%20Value%20Of%20Privacy.pdf (last visited Apr. 2, 2018).

product based on its set of attributes."[5] The results of such discrete choice experiments demonstrate damages when certain privacy expectations have been invaded.

42. Among other ways to demonstrate damages resulting from violation of BIPA, such discrete choice experiments can be applied to an employer's capturing, collecting, storing, and/or disseminating employees' biometric information without their consent, such as is the case here.

43. Moreover, the Illinois legislature quantified damages for BIPA violations by expressly providing for "liquidated damages" as compensation under the Act.

44. In addition to the quantifiable injury that results when privacy expectations such as those protected by BIPA are violated, unwanted invasions of privacy also result in increased risk of harm to victims. Ginger Jin, former Director of the FTC's Bureau of Economics, recently noted this reality when advocating for an *ex-ante* perspective on informational injury because of the limitations of measuring such injury from an *ex-post* perspective:

> One crucial question is whether we should measure consumer harm in ex-ante or ex-post perspective. . . . The ex-post perspective is quite intuitive. Somebody misused consumer's information that results in, say, an identity theft or a fraudulent transaction. We can measure that by the amount of time, money, and effort that consumer's lost because of this.

---

[5] Sarah Butler & Garrett Glasgow, Ph.D., *The Value of Personal Information to Consumers of Online Services: Evidence from a Discrete Choice Experiment* (June 19, 2014), *available at* http://www.nera.com/content/dam/nera/publications/archive2/PUB_Value_Personal_Info_0714.pdf (last visited Apr. 2, 2018).

> However, the ex-post perspective, I would argue, is narrow-minded, because a lot of harm may not happen yet, but there's a risk there. . . .
>
> I would argue that, in fact, [placing] emphasis on ex-post harm . . . ends up encouraging overuse or misuse of data, [companies] don't need to account to the negative [externality] they are imposing on consumers. So in my view, that's inadequate.[6]

45. Ms. DeMooy echoed Ms. Jin's thoughts, explaining that from the very moment of collection of personal information without consent, "that is where the risk [to the consumer] is raised. [And] that means that [the consumer's] risk for identification, his risk for all of the other harms that come later, has been elevated."[7]

46. Importantly, the above injury from unwanted capture, collection, storage, and use—as well as the risk of further injury posed by such actions—is greater when the information affected is highly sensitive, immutable personal information such as biometrics. For example, as Ms. DePooy has explained, personal health information "raises more risk in terms of harm" because it is "not information we can replace easily. It's not information that can go somewhere else. It is immutable and intrinsic and inherent to us."[8]

47. Given the prevalence of data breaches and the sensitivity of biometric information, the immediate harm of unauthorized collection is irrefutable. As explained in a recent article by the New York Times:

> Hacking of banks and identities is big business. An estimated 17.6 million Americans were subject to identity theft in

---

[6] FTC Informational Injury Workshop (Panel 4 – Measuring Injury) (Dec. 12, 2017), *available at* https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-4-measuring-injury (last visited Apr. 2, 2018).
[7] *Id.*
[8] *Id.*

> 2014, mostly through breached bank accounts and credit cards. At this point, bank hackers are probably not looking for biometric data when attacking a bank. But even if it leaks as a by-product of a financial breach, criminals will find ways to abuse biometric data or resell it for further exploitation. And biometric data is more sensitive than other personal information banks store on behalf of their customers because, unlike a credit card number (or even a name!), stolen biometric data cannot be replaced: It corresponds to a patient's face or fingerprints. . . .
>
> If the compromised data happens to be biometrics, issues of identity theft may simply be unresolvable. . . . It is not enough for banks to simply avoid storing images of fingerprints, faces or irises. The biometric data that they get from processing those geometrics (what banks call "templates") can also be abused if they are accessed in combination with the algorithm used to extract the templates from the original images.[9]

48. Even the U.S. Office of Personnel Management suffered a data breach which resulted in the theft of more than 5 million employees' fingerprints by agents of a foreign state. In response, the federal government encouraged victims to obtain biometric identity theft protection services to prevent unauthorized use of their biometrics.

49. In short, the harm to persons whose rights under BIPA have been violated is recognized, concrete, and quantifiable.

V. Defendant Has Repeatedly Violated Plaintiffs' BIPA Rights

50. At all relevant times, Plaintiffs worked for Southwest at Chicago Midway International Airport.

[9] Yana Welinder, "Biometrics in Banking Is Not Secure," THE N.Y. TIMES, July 13, 2016, *available at* https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-in-banking-is-not-secure (last visited Apr. 2, 2018).

51. Plaintiffs were required to provide their biometric identifiers and/or biometric information to Defendant so that Defendant could operate its biometric timekeeping system and identify Plaintiffs in the future for timekeeping and payroll purposes.

52. Thereafter, Defendant required Plaintiffs to scan their finger into one of Defendant's biometric timekeeping devices, at a minimum, each time they "clocked-in" and "clocked-out" of work. Defendant's system ensures that workers can only verify their attendance and timeliness through scanning such biometric information.

53. Accordingly, in addition to the occasion when Defendant initially captured workers' fingerprints, Defendant captured and used Plaintiffs and other workers' fingerprints in violation of BIPA on each occasion that Defendant required its workers in Illinois to scan a finger through Defendant's biometric timekeeping devices.

54. As a result, Plaintiffs' biometric information is and has been associated with their identities and has been used by Defendant to identify and track their work time.

55. Prior to obtaining Plaintiffs' biometric identifiers and/or biometric information, Defendant did not inform Plaintiffs in writing that a biometric identifier or biometric information was being captured, collected, stored, or used, nor did Defendant make its policy about collection, retention, and use of such information publicly available as required by BIPA.

56. Prior to taking Plaintiffs' biometric identifiers and/or information, Defendant did not make a written policy available to its workers or to the public establishing a retention schedule and guidelines for permanently destroying the biometric identifiers and biometric information that it collects, as required by BIPA.

57. Additionally, Defendant did not obtain consent for any transmission to third parties of Plaintiffs' and other employees' biometrics. To the extent Defendant utilizes out of state vendors to operate its biometrics program in conformance with biometric industry practice, Defendant has also violated BIPA on each occasion it transmits such information to third parties.

58. To this day, Plaintiffs are unaware of the status of their biometric information that was taken by Defendant. Defendant has not informed Plaintiffs whether it still retains their biometric information, and if it does, for how long it intends to retain such information without their consent.

59. Defendant does not have a policy of informing its workers in any way what happens to their biometric information after it is captured, collected, and obtained, whether the information is transmitted to a third party and, if so, which third party, and what would happen to the information if an individual discontinues working for Defendant, if a facility were to close, or if Defendant was to be acquired, sold, or file for bankruptcy.

60. Given the invasive nature of Defendant's timekeeping system as well as the risks attendant to providing biometric information to Defendant, Plaintiffs were not sufficiently compensated by Defendant for the capture, collection, storage,

retention, and/or use of their biometric information. Plaintiffs would not have agreed to work for Defendant, at least not for the compensation they received, had they been informed pursuant to BIPA of the of the nature of Defendant's biometric timekeeping system.

61. By knowingly and willfully failing to comply with BIPA's mandatory notice, written release, and policy publication requirements, Defendant has violated Plaintiffs' and other workers' substantive privacy rights under BIPA. Defendant has also violated Plaintiffs' and other workers' rights under the common law.

62. Plaintiffs and the other members of the class have continuously been exposed to substantial and irreversible loss of privacy by Defendant's retention of their biometric information without their consent, with such constant and ongoing exposure constituting a severe harm and violation of their rights.

63. On behalf of themselves and the proposed class defined below, Plaintiffs seek an injunction requiring Defendant to destroy the Class member's biometrics in Defendant's possession, to cease all unlawful activity related to the capture, collection, storage, and use of their and other class member's biometrics and an award of statutory damages to the class members, together with costs and reasonable attorneys' fees, as well as other damages enumerated below.

CLASS ALLEGATIONS

64. Plaintiffs bring this action on behalf of themselves and similarly situated individuals pursuant to Federal Rule of Civil Procedure 23. Plaintiffs seek to represent a class ("Class") defined as follows:

> All individuals whose biometrics were captured, collected, obtained, stored or used by Defendant within the State of Illinois at any time within the applicable limitations period.

65. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

66. Upon information and belief, there are hundreds, if not thousands, of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiffs, the members can easily be ascertained through Defendant's personnel records.

67. Plaintiffs' claims are typical of the claims of the Class members they seek to represent because the factual and legal bases of Defendant's liability to Plaintiffs and the other Class members is the same, and because Defendant's conduct has resulted in similar injuries to Plaintiffs and to the Class. As alleged herein, Plaintiffs and the other putative Class members have all suffered damages as a result of Defendant's BIPA violations as well as violations of the common law.

68. There are many questions of law and fact common to the claims of Plaintiffs and the other Class members, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant collects, captures, stores, or uses the biometrics of Class members;

b. Whether Defendant developed and made available to the public a written policy that establishes a retention schedule and guidelines for permanently destroying biometric identifiers and information as required by BIPA;

c. Whether Defendant obtained a written release from Class members before capturing, collecting, or otherwise obtaining workers' biometrics as required by BIPA;

d. Whether Defendant provided a written disclosure to its workers that explains the specific purposes, and the length of time, for which their biometrics were being collected, stored and used before taking their biometrics as required by BIPA;

e. Whether Defendant's conduct violates BIPA;

f. Whether Defendant's violations of BIPA are willful and reckless;

g. Whether Defendant intruded upon Class members' seclusion when it captured, collected, stored, and/or otherwise used Class members' biometric information;

h. Whether Defendant converted Class members' private property when it captured, collected, stored, and/or otherwise used Class members' biometric information;

i. Whether Defendant's capture, collection, storage, and/or use of Class members' biometric information was negligent;

j. Whether Defendant breached an express or implied agreement to comply with BIPA and/or treat Class members' biometric information lawfully when it captured, collected, stored, and/or otherwise used Class members' biometric information;

k. Whether Defendant's capture, collection, storage, and/or use of Class members' biometric information resulted in a benefit to Defendant to the detriment of Class members and whether the retention of such a benefit is inequitable; and

l. Whether Plaintiffs and the Class members are entitled to damages and injunctive relief.

69. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

70. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class they seek to represent. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

71. Defendant has acted and failed to act on grounds generally applicable to the Plaintiffs and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*., (on behalf of Plaintiffs and the Class)

72. Plaintiffs incorporate paragraphs 1-71 above as if fully restated herein.

73. BIPA makes it unlawful for private entities to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of time for which a biometric identifier or biometric information is being captured, collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

74. Illinois' BIPA also requires that private entities in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. Entities which possess biometric identifiers or information must (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric information (entities may not retain biometric information longer than three years after the last interaction with the individual); and (ii) must adhere to the publicly posted retention and deletion schedule. 740 ILCS 14/15(a)

75. Defendant is a "private entity" as that term is defined under BIPA. 740 ILCS 14/10.

76. Plaintiffs and the Class members have had their "biometric identifiers," namely their fingerprints, collected, captured, received or otherwise obtained by Defendant. Plaintiffs and the other Class members' biometric identifiers were also

used to identify them, and therefore constitute "biometric information" as defined by BIPA. 740 ILCS 14/10.

77. Each instance Plaintiffs and the other Class members scanned their fingerprints into Defendant's timekeeping devices, Defendant captured, collected, stored, and/or used Plaintiffs' and the Class members' biometric identifiers or biometric information without valid notice or consent and, therefore, in violation of BIPA.

78. Defendant's practice of capturing, collecting, storing, and using biometric identifiers and biometric information fails to comply with applicable BIPA requirements. Specifically, with respect to Plaintiffs and the other Class members, Defendant failed to:

a. Obtain the written release required by 740 ILCS 14/15(b)(3);

b. Inform Plaintiffs and the Class members in writing that their biometric identifiers and/or biometric information were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(1);

c. Inform Plaintiffs and the Class in writing of the specific purpose for which their biometric information and/or biometric identifiers were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

d. Inform Plaintiffs and the Class in writing of the specific length of term their biometric information and/or biometric identifiers were

being captured, collected, stored and used, as required by 740 ILCS 14/15(b)(2); and

e. Provide a publicly available retention schedule detailing the length of time biometric information is stored and guidelines for permanently destroying the biometric information it stores, as required by 740 ILCS 14/15(a).

79. By capturing, collecting, storing, and using Plaintiffs' and the other Class members' biometric identifiers and/or biometric information as described herein, Defendant violated Plaintiffs' and the other Class members' respective rights to privacy as set forth in BIPA. 740 ILCS 14/15(a).

80. BIPA provides for statutory liquidated damages of $5,000 for each willful and/or reckless violation and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1).

81. Defendant's violations of BIPA, as set forth herein, were knowing and willful, or were in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with the BIPA disclosure, consent, and policy posting requirements.

COUNT II
Intrusion Upon Seclusion
(on behalf of Plaintiffs and the Class)

82. Plaintiffs incorporate paragraphs 1-81 above as if fully restated herein.

83. Defendant has intentionally and unlawfully intruded upon Plaintiffs' and the Class members' private affairs and concerns by using biometric scanning

devices to physically collect their biometrics without receiving consent in violation of the law.

84. On information and belief, Defendant has intentionally and unlawfully intruded upon Plaintiffs' and the Class members' private affairs and concerns by disseminating their biometrics to unknown third parties, such as payroll vendors or timekeeping vendors, without knowledge or consent in violation of the law.

85. Plaintiffs and the Class members had a reasonable expectation that their biometric information would not be captured, collected, stored, and/or used by their employer. Moreover, Plaintiffs and Class members had a reasonable expectation that any entity seeking to collect and use their biometrics, and particularly their employer, would be doing so in accordance with the law.

86. A reasonable person would find it highly offensive and objectionable that an entity would intrude on their highly sensitive and irreplaceable biometrics in violation of the law and without legal consent. Plaintiffs and the Class members did find, and continue to find, Defendant's conduct to be both highly offensive and objectionable.

87. Defendant's repeated intrusion upon Plaintiffs' and Class members' seclusion caused damages to Plaintiffs and Class members in the form of, among other things, mental anguish and suffering. Plaintiffs and the Class members therefore seek monetary damages and restitution in an amount to be determined at trial.

COUNT III
Conversion
(on behalf of Plaintiffs and the Class)

88. Plaintiffs incorporate paragraphs 1-87 above as if fully restated herein.

89. Plaintiffs and Class members have a right to exclusive possession of their biometric information.

90. Plaintiffs and Class members have a right to absolute and immediate possession of their biometric information from Defendant in particular.

91. Nonetheless, Defendant wrongfully and without authorization assumed control, dominion, and/or ownership over Plaintiffs' biometric information by capturing, collecting, storing, and/or using it as a part of Defendant's timekeeping and payroll practices.

92. Any demand by Plaintiffs and Class members for immediate possession of their biometric information from Defendant would have been futile. In any event, Defendant had sold, disposed of, and/or fundamentally changed the biometric information at issue by capturing, collecting, storing, and/or disseminating it without Plaintiffs' and Class members' permission.

93. As a direct and proximate result of Defendant's actions, Plaintiffs and Class members have been damaged in an amount to be determined at trial.

COUNT IV
Negligence
(on behalf of Plaintiffs and the Class)

94. Plaintiffs incorporate paragraphs 1-93 above as if fully restated herein.

95. By requiring that Plaintiffs and Class members provide their biometric information and by capturing, collecting, storing, and/or otherwise using such

biometric information, Defendant owed a duty of ordinary care to Plaintiffs and Class members.

96. Defendant breached that duty to Plaintiffs and Class members by: (a) failing to abide by BIPA with respect to Plaintiffs' and Class members' biometric information; (b) negligently capturing, collecting, and storing such biometric information; and/or (c) negligently disseminating such biometric information to third-party vendors to the extent Defendant operates according with industry payroll practices.

97. As a direct and proximate result of Defendant's breach of duty, Plaintiffs and Class members have sustained damages in an amount to be proved at trial.

COUNT V
Fraud (in the alternative to Count IV)
(on behalf of Plaintiffs and the Class)

98. Plaintiffs incorporate paragraphs 1-93 as if fully restated herein.

99. Defendant intentionally concealed and/or omitted the nature and extent of its capture, collection, storage, and/or use of Plaintiffs' and Class members' biometric information in order to induce Plaintiffs and Class members to provide such biometric information to Defendant. Such concealed information was material to Plaintiffs and Class members as it would be to any reasonable person in deciding whether to provide their biometric information to a third party.

100. Defendant's concealment and/or omission was intended to induce the belief of Plaintiffs and Class members that: (a) they were not providing to Defendant immutable personal information; (b) Defendant was not capturing, collecting, storing,

and/or using their immutable personal information; and/or (c) that they were not exposing their immutable personal information to dissemination to third parties and/or the risk of theft.

101. Because Defendant was Plaintiffs' and Class members' employer and/or because of Defendant's statutory duties under BIPA, Defendant had a duty to disclose to Plaintiffs and Class members the nature and extent of the biometrics it collected, how such biometrics would be used and/or disseminated, and the risks therefrom.

102. Plaintiffs and Class members relied upon Defendant's silence as a representation that: (a) they were not providing to Defendant immutable personal information; (b) Defendant was not capturing, collecting, storing, and/or using their immutable personal information; and/or (c) that they were not exposing their immutable personal information to dissemination to third parties and/or the risk of theft. In the alternative, Plaintiffs and Class members could not have discovered such facts through reasonable inquiry or inspection or were prevented from making such a reasonable inquiry or inspection because Defendant maintained total control over information relating to its timekeeping program and its collection, capture, storage, and/or use of biometric information.

103. Had Plaintiffs and Class members been aware of such material information concealed and/or omitted by Defendant, they would not have accepted or continued employment, or at least would not have accepted or continued employment without additional compensation.

104. As such, Plaintiffs and Class members were damaged by their reliance on Defendant's fraudulent concealment and/or omission in an amount to be proved at trial.

COUNT VI
Breach of Contract (in the alternative to Counts II-V)
(on behalf of Plaintiffs and the Class)

105. Plaintiffs incorporate paragraphs 1-71 above as if fully restated herein.

106. In the alternative to Counts II-V above, as a part of implementing its biometric timekeeping system, Defendant in word and/or in actions expressly or impliedly agreed to: (a) adhere to the law when capturing, collecting, and/or storing Plaintiffs' and Class members' biometric identifiers and/or biometric information; and (b) not disseminate such biometric information to third parties and/or expose such biometric information to risk of theft. Defendant agreed as to the foregoing in return for Plaintiffs and Class members providing their biometric identifiers and/or information and subjecting themselves to Defendant's timekeeping system.

107. Plaintiffs and Class members provided their biometric identifiers and/or information to Defendant and participated in Defendant's biometric timekeeping system. Accordingly, Plaintiffs and Class members performed all requisite promises and/or acts under the foregoing agreement with Defendant.

108. Defendant breached the above agreement with Plaintiffs and Class members by: (a) failing to adhere to the law when capturing, collecting, and/or storing Plaintiffs' and Class members' biometric information; and/or (b) disseminating such biometric information to third parties to the extent Defendant

follows industry payroll practices and/or exposing such biometric information to the risk of theft.

109. As a direct and proximate result of Defendant's breach, Plaintiffs and Class members have sustained monetary damages in an amount to be determined at trial.

COUNT VII
Breach of Contract Implied in Law (in the alternative to Count VI)
(on behalf of Plaintiffs and the Class)

110. Plaintiffs incorporate paragraphs 1-104 above as if fully restated herein.

111. In the alternative to Count VI above, requiring that Plaintiffs and Class members provide their biometric identifiers and/or biometric information and participate in Defendant's biometric timekeeping system, Defendant retained a benefit in the form of cost savings, increased profit, and/or increased worker productivity (achieved through eliminating timekeeping mistakes, for example).

112. Defendant's benefit occurred to the detriment of Plaintiffs and Class members in that Plaintiffs' and Class members' substantive privacy rights were violated in the process. Such privacy rights were violated in that: (a) Plaintiffs' and Class members' biometric identifiers and/or biometric information was captured, collected, stored, and/or used without their knowledge, notice, or written consent and without being provided a plan for the treatment of such information; and (b) Plaintiffs and Class members were unjustly exposed to greater risk of injury as a result of Defendant's practices with respect to their biometrics.

113. Defendant's retention of the foregoing cost-savings and profits to the detriment of Plaintiffs and Class members violates the fundamental principles of justice, equity, and good conscience.

114. Accordingly, Plaintiffs and Class members have sustained damages in the amount of Defendant's profits and cost-savings, among other damages, in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, respectfully request that this Court enter an Order:

a. Certifying the Class as defined above, appointing Plaintiffs as class representatives and the undersigned as class counsel;

b. Declaring that Defendant's actions, as set forth herein, violate the BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with the BIPA requirements for the capture, collection, storage, and use of biometric identifiers and biometric information, including an injunction requiring Defendant to permanently destroy all biometric information of Plaintiffs and of Class members in its possession and compensation in an amount to be determined at trial for the commercial value of Plaintiffs' biometric information;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(1);

e. Awarding statutory damages of $1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(3);

f. Awarding reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);

g. Awarding damages for mental anguish and suffering as set forth in Count II;

h. Awarding monetary damages for Defendant's violations as set forth in Counts III-VI;

i. Awarding damages in the form of Defendant's profits and/or cost-savings as set forth in Count VII;

j. Awarding pre- and post-judgment interest, as allowable by law; and

k. Awarding such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiffs requests trial by jury in this action on each and every one of their claims.

Dated: April 2, 2018

Respectfully Submitted,

HART MCLAUGHLIN & ELDRIDGE, LLC

By: /s/ *Steven A. Hart*
One of the Attorneys for Plaintiffs and the Class

Steven A. Hart
Robert J. McLaughlin
Brian H. Eldridge
Kyle Pozan
John S. Marrese
HART MCLAUGHLIN & ELDRIDGE, LLC
121 W. Wacker Drive, Suite 1050
Chicago, Illinois 60601
Tel: (312) 955-0545
Fax: (312) 971-9243
shart@hmelegal.com
rmclaughlin@hmelegal.com
beldridge@hmelegal.com
kpozan@hmelegal.com
jmarrese@hmelegal.com

Antonio M. Romanucci
ROMANUCCI & BLANDIN, LLC
321 N. Clark Street, Suite 900
Chicago, Illinois 60654
Tel: (312) 458-1000
Fax: (312) 458-1004
aromanucci@rblaw.net

Attorneys for Plaintiffs and the Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that, on April 2, 2018, he caused a true and correct copy of the foregoing **Amended Class Action Complaint** to be electronically filed with the Court, a copy of which will be automatically served on all parties by operation of the Court's electronic filing system.

/s/ *Steven A. Hart*